Computer Security and Cryptography

CS381

来学嘉

计算机科学与工程系 电院3-423室

34205440 1356 4100825 laix@sjtu.edu.cn

2015-05

Organization

- Week 1 to week 16 (2015-03 to 2014-06)
- 东中院-3-102
- Monday 3-4节; week 9-16
- Wednesday 3-4节; week 1-16
- lecture 10 + exercise 40 + random tests 40 + other 10
- Ask questions in class – counted as points
- Turn ON your mobile phone (after lecture)
- Slides and papers:
  - http://202.120.38.185/CS381
    - computer-security
  - http://202.120.38.185/references
- TA: Geshi Huang gracehgs@mail.sjtu.edu.cn
- Send homework to the TA

Rule: do the homework on your own!

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions and MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking
- Computer and network security
  - Access control
  - Malware
  - Firewall
- Examples: Flame, Router, BitCoin ??

References

- W. Stallings, *Cryptography and network security - principles and practice*， Prentice Hall.
- W. Stallings, 密码学与网络安全：原理与实践（第4版），刘玉珍等译，电子工业出版社，2006
- Lidong Chen, Guang Gong, *Communication and System Security*, CRC Press, 2012.
- A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997, ISBN: 0-8493-8523-7, http://www.cacr.math.uwaterloo.ca/hac/index.html
- B. Schneier, *Applied cryptography*. John Wiley & Sons, 1995, 2nd edition.
- 裴定一,徐祥, 信息安全数学基础, ISBN 978-7-115-15662-4, 人民邮电出版社,2007.

contents

- Public-key cryptosystems:
  - RSA - factorization
  - DH , ElGamal -discrete logarithm
  - ECC
- Math
  - Fermat's and Euler's Theorems & ø(n)
  - Group, Fields
  - Primality Testing
  - Chinese Remainder Theorem
  - Discrete Logarithms

Group

- a set G, and • : $G \times G \rightarrow G$ be a binary operation, satisfying
  - closure: for $a,b \in G$, $a \bullet b \in G$;
  - associativity: for $a,b,c \in G$,
    $(a \bullet b) \bullet c = a \bullet (b \bullet c)$;
  - (identity) There is an element $e \in G$, such that for any $a \in G$, $e \bullet a = a \bullet e = a$
  - (Inverse) For any $a \in G$, there exists an element $b \in G$, such that, $a \bullet b = b \bullet a = e$.

  Then $(G, \bullet)$ is called to be a group.
- A group $(G, \bullet)$ is an Abelian group if it also satisfy
  - (Commutativity) For any $a,b \in G$, $a \bullet b = b \bullet a$.

Eample.

- (Z, +), (Q, +), (R, +); $(Z_m, +)$
- $(Z^* = Z \setminus \{0\}, \bullet)$, $(Z_P^*, \bullet)$

Cyclic group

- Order of an element：for $a \in G$, compute $\{a, a^2, \ldots, a^m=1\}$， the least positive integer m such that $a^m=1$ is called to be the order of *a*.
- $\{1, a, a^2, \ldots, a^{m-1}\}$ is a cyclic group with order *m. a* is called the generator of the cyclic group.
- Lemma: if the order of a is m and if $a^n=1$， then $m|n$.
- Lemma: if the order of a is m, then the order of a^k is $m/\gcd(k,m)$.
- Theorem: if the order of group *G* is *n*, then for any subgroup of G， the order of subgroup divides *n*.
- **Cyclic subgroups of (Z_7^*, •)**
  - **$1^0=1$** **{1}**
  - **$2^0=1, 2^1=2, 2^2=4, 2^3=1$** **{1,2,4}**
  - **$3^0=1, 3^1=3, 3^2=2, 3^3=6, 3^4=4, 3^5=5, 3^6=1$** **{1,3,2,6,4,5}**
  - **$4^0=1, 4^1=4, 4^2=2, 4^3=1$** **{1,2,4}**
  - **$5^0=1, 5^1=5, 5^2=4, 5^3=6, 5^4=2, 5^5=3, 5^6=1$** **{1,5,4,6,2,3}**
  - **$6^0=1, 6^1=6, 6^2=1$** **{1,6}**

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Field

- Let F be a set, and • and + are binary operations defined over F, satisfying
  - (F,+) is an Abelian additive group with identity 0;
  - (F\{0}, •) is a multiplicative group, with identity 1;
  - Distributive law: For any $a,b,c \in F$: $a \bullet (b+c)=a \bullet b+ a \bullet c$

(F,+, •) is called to be a field.

Example: let p be a prime, then (Z_p,+, •) is a field, called Galois Field, denoted as $GF(P)=F_p$.

Galois,

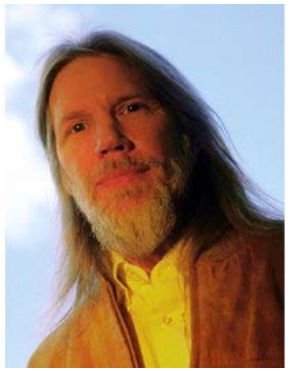
1811～1832

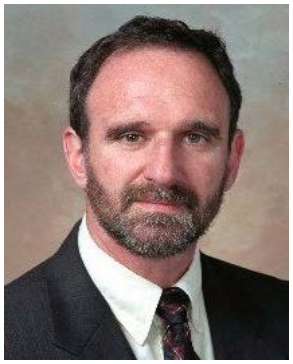
Discrete logarithm

- For any 0<*x*<*p* in GF(*p*).
  - Given *x* and *g*, compute $y \equiv g^x \pmod{p}$ is called modular exponentiation,
  - Given *g* and *y*, to find *x* such that $y \equiv g^x \pmod{p}$ is called discrete logarithm, written as $x = log_g\, y \ (mod\ p)$
- exponentiation is relatively easy, with computation complexity $O(\log_2(p))$。
- finding discrete logarithms is generally a **hard** problem

Diffie-Hellman Key Agreement

W.Diffie and M.E.Hellman, “New Directions in Cryptography”, IEEE Transaction on Information Theory, V.IT-22.No.6, Nov 1976, PP.644-654





Parameters: p, g

Alice

Choose a

Compute $g^a \bmod p$

$g^a \bmod p$ →

← $g^b \bmod p$

Compute $g^{ab} \bmod p$

Bob

Choose b

Compute $g^b \bmod p$

Compute $g^{ab} \bmod p$

g^{ab} is the secrete key shared by Alice and Bob

ElGamal encryption algorithm

- Set up: $\mathrm{GF}(p)$, and g the primitive element.
- Users' key generation:
  - user U randomly chooses $x \in \mathrm{GF}(p)^*$ as his private key.
  - Compute $y \equiv g^x \pmod p$ as his public key.
- Encryption: suppose that Alice wants to send Bob a message $m \in \mathrm{GF}(p)$. She uses Bob's public key y_b,
  - Alice randomly chooses an integer r, and compute $R = g^r$
  - Alice computes $S = m \cdot y_b^r \pmod p$;
- Alice sends (R,S) to Bob
- Decryption: Bob uses his own private key to decrypt m from (R,S) : $m = S/R^{x_b} = (m \cdot y_b^r)/(g^r)^{x_b}$

ElGamal encryption algorithm

Alice sends Bob a message $m \in$ GF(p). Using Bob's public key

Parameters: p, g

Alice $SK_A=(x_A)$

$PK_A=(y_A) = (g^{xA} \bmod p)$

Bob $SK_B=(x_B)$

$PK_B=(y_B) = (g^{xB} \bmod p)$

Get PK_B,

Compute $R=g^r \bmod p$

Compute $S=m\, y_B^{\,r} \bmod p$

(R,S)

$m = S/R^{x_b} = (m \bullet y_b^{\,r})/(g^r)^{x_b}$

Compute $m=S/R^{xB} \bmod p$

ElGamal Signature Algorithm

- Parameters are chosen as in encryption algorithm.
  - Alice's private key is x_a, and public key is $y_a=g^{x_a}$
  - Bob's private key is x_b, and public key is $y_b=g^{x_b}$
- Signing
  - Alice randomly chooses an integer r *such that* $\gcd(r, p-1)=1$, and gets $R=g^r$
  - Alice uses her own private key x_a to compute

$$S=r^{-1}(m-x_aR) \pmod{p-1}$$

- Alice sends (m, R, S) to Bob
- Verification
  - Bob verifies $g^m=y_a^R R^S \pmod{p}$

ElGamal Signature Algorithm

Parameters: p, g

Alice $SK_A = x_A$

$PK_A = y_A = (g^{xA} \bmod p)$

Bob $SK_B = x_B$

$PK_B = y_B = (g^{xB} \bmod p)$

Choose r, *such that* $\gcd(r, p-1)=1$

Compute $R = g^r \bmod p$

Compute $S = r^{-1}(m - x_A R) \bmod p-1$

(m, R, S) →

Verify $g^m = y_A{}^R R^S \bmod p$

Complexity of Dlog

- Similar to factoring large number n, for discrete logarithm, the complexity of currently known algorithms is about

  $\exp(b^{1/3} \log^{2/3}(b))$ $b=\log(p)$ (number field sieve)

- b should be at least 1024 bit

- Use strong prime: p-1 has large factors.

Chinese Remainder Theorem

- Find a number x that leaves
  - a remainder of 2 when divided by 3,
  - a remainder of 3 when divided by 5,
  - a remainder of 4 when divided by 7.
- If

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod 7$$

- x=?

Chinese Remainder Theorem

- Let $(n_1, n_2,\ldots,n_k)$ be pairwise relatively prime positive integers. Then the system of congruence
  - $x \equiv a_1 \pmod{n_1}$
  - $x \equiv a_2 \pmod{n_2}$
  - ……
  - $x \equiv a_k \pmod{n_k}$

  has a unique solution (modulo $n_1 n_2 \ldots n_k$)
- Solution

$n=n_1 n_2 \ldots n_k$, $m_i=n/n_i$, $m_i' = m_i^{-1} \pmod{n_i}$

$x=a_1 m_1 m_1' + a_2 m_2 m_2' + \ldots + a_k m_k m_k'$

Chinese Reminder Theorem (CRT)

Theorem

Let n_1, n_2, ,,, n_k be integers s.t. gcd(n_i, n_j) = 1 for any $i \neq j$.

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\ldots$$

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo $n = n_1 n_2 \ldots n_k$

Proof of CRT

- Consider the function χ: $Z_n \rightarrow Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$
  $\chi(x) = (x \bmod n_1, \ldots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \le i \le k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i) = 1$
- For $1 \le i \le k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a1,a2,\ldots,ak) = \sum a_i m_i y_i \bmod n$, this function inverts χ
  - $a_i m_i y_i \equiv a_i \pmod{n_i}$
  - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

An Example Illustrating Proof of CRT

- Example of the mappings:
  - $n_1=3$, $n_2=5$, $n=15$
  - $m_1=5$, $y_1=m_1^{-1} \bmod n_1=2$, $5 \cdot 2 \bmod 3 = 1$
  - $m_2=3$, $y_2=m_2^{-1} \bmod n_2=2$, $3 \cdot 2 \bmod 5 = 1$
  - $\rho(2,4) = (2 \cdot 5 \cdot 2 + 4 \cdot 3 \cdot 2) \bmod 15$
    $= 44 \bmod 15 = 14$
  - $14 \bmod 3 = 2$, $14 \bmod 5 = 4$

Solve $a^x \equiv b \pmod p$

An exhaustive search for all $0 \le x < p$

- Check only for even x or odd x according to $b^{(p-1)/2} \equiv (a^x)^{(p-1)/2} \equiv (a^{(p-1)/2})^x \equiv (-1)^x \equiv 1$ or -1 (mod p), where a is a primitive root

(Ex) p=11, a=2, b=9, since $b^{(p-1)/2} \equiv 9^5 \equiv 1$,

then check for even numbers {0,2,4,6,8,10}

only to find x=6 such that $2^6 \equiv 9 \pmod{11}$

Attack when p-1 consists of small primes

- Suppose p-1=2^n， a is a generator of Z_p*
- Given $b=a^x \bmod p$, to compute x=?
  - Let $x=2^{n-1}x_{n-1}+\ldots+2x_1+x_0$
  - If $b^{2^{n-1}}=1$, then $x_0=0$; if $b^{2^{n-1}}=-1$, then $x_0=1$.
  - Compute $b_1=b/a^{x_0}$
  - If $b_1^{2^{n-2}}=1$, then $x_1=0$, if $b_1^{2^{n-2}}=-1$, then $x_1=1$.
  - Compute $b_2=b_1/a^{2x_1}$
  - …
  - If $b_{n-1}=1$, then $x_{n-1}=0$, if $b_{n-1}=0$ then $x_{n-1}=1$

Solve $a^x \equiv b \pmod p$ by Pohlig-Hellman

Works if p-1 can be factorized into small numbers, i.e.,

p-1=$q_1 q_2 \ldots q_r$

For every factor q|(p-1), do the following:

write $b_0 = b$, and, $x = x_0 + x_1 q + x_2 q^2 + \cdots + x_{r-1} q^{r-1}$ for $0 \le x_i \le q-1$

1. Find $0 \le k \le q-1$ such that $(a^{(p-1)/q})^k \equiv b^{(p-1)/q} \bmod p$,
   then $x_0 \equiv k$, next let $b_1 \equiv b_0 a^{-x0}$
2. Find $0 \le k \le q-1$ such that $(a^{(p-1)/q})^k \equiv [b_1]^{(p-1)/q\wedge 2}$, then $x_1 \equiv k$, nex
   let $b_2 \equiv b_1 a^{-x1}$
3. Repeat steps 1, 2 until x_{r-1} is found
4. Repeat steps 1~3 for all q's, then apply Chinese Remainder
   Theorem to get the final solution

The correctness of Pohlig-Hellamn

Let $a^x \equiv b$. For every factor $q|(p-1)$,

write $x=x_0 + x_1q + x_2q^2 + \cdots + x_{r-1}q^{r-1} = x_0+wq$.

If we could find $0 \le k \le q-1$ such that $(a^{(p-1)/q})^k \equiv b^{(p-1)/q} \bmod p$,

then $x_0 \equiv k$.

Proof. $b^{(p-1)/q} \equiv (a^x)^{\frac{p-1}{q}} \equiv (a^{p-1})^w a^{\frac{x_0(p-1)}{q}}$

$$\equiv \left(a^{\frac{p-1}{q}}\right)^{x_0} \bmod p$$

$7^x \equiv 12 \pmod{41}$; p=41, a=7, b=12,

- p-1=41-1=40 $=2^3 5$
- $b_0 = 12$
- For q=2: $b_0 = 12$, $b_1 = 31$, $b_2 = 31$, and
  $x = x_0 + 2x_1 + 4x_2 \equiv 1 + 2 \cdot 0 + 4 \cdot 1 \equiv 5 \pmod 8$
- For q=5: $b_0 = 12$, $b_1 = 18$, and
  $x = x_0 \equiv 3 \pmod 5$

Solving $x \equiv 5 \pmod 8$ and $x \equiv 3 \pmod 5$,

We have $x \equiv 13 \pmod{40}$

Primality Testing

- often we need to find large prime numbers
- traditionally **sieve** using **trial division**
  - i.e. divide by all numbers (primes) in turn less than the square root of the number
  - only works for small numbers
- alternatively can use statistical primality tests based on properties of primes
  - for which all primes numbers satisfy property
  - but some composite numbers, called pseudo-primes, also satisfy the property
- can use a slower deterministic primality test

Some facts about primes

- Any positive odd $n \geq 3$ can be written as

  $n - 1 \geq 2^k q$ for q>0 and odd q

Fact 1. For any prime p and any number 0<a<p,

$a^2 \equiv 1 \, mod \, p$ if and only if $a \equiv 1 \, mod \, p$ or $a \equiv -1 \, mod \, p$

Fact 2. Let $p = 2^k q + 1$ be an odd prime number for odd q, and let 1<a<p-1. Then one of the following two is true.

1. $a^q \equiv 1 \, mod \, p$ 2. $\exists b \in \{a^q, a^{2q}, \cdots, a^{2^{k-1}q}\}$: $b \equiv -1 \, mod \, p$

Proof. Fermat's Theorem: $a^{2^k q} = a^{p-1} \equiv 1 \, mod \, p$

Consider $a^q, a^{2q}, \cdots, a^{2^{k-1}q}$ either 1 or 2 holds.

Miller Rabin Algorithm

- based on Fermat's Theorem: $a^{p-1} = 1 \pmod p$
- TEST (*n*):
  1. Find integers *k*, *q*, *k* > 0, *q* odd, so that $(n-1)=2^k q$
  2. Select a random integer a, $1<a<n-1$
  3. **if** $a^q \bmod n = 1$ **then** return ("inconclusive");
  4. **for** *j* = 0 **to** *k* – 1 **do**
     5. **if** $(a^{2^j q} \bmod n = n-1)$
        then return("inconclusive")
  6. return ("composite")
- Prob(inconclusive but p not prime) < ¼ [KNUT98]
  - repeat test with different random a
  - Prob(n is prime after *t* tests) = $1-4^{-t}$ (0.99999 for t=10)

Summary

- Public-key cryptosystems:
  - RSA - factorization
  - DH , ElGamal -discrete logarithm
  - ECC
- Math
  - Fermat's and Euler's Theorems & ø(n)
  - Group, Fields
  - Primality Testing
  - Chinese Remainder Theorem
  - Discrete Logarithms

Exercise 9 – PKC

1. If x=2 (mod 3) x=3 (mod 5) x=4 (mod 7), what is x?
2. compute $\phi(24)$=#{ ? }, and $\phi(n)$ for $n=p_1^{e1} p_2^{e2} p_3^{e3}$
3. Prove：in ElGamal Signature Algorithm, the Verification test $g^m=y_a^R R^S \pmod p$ is valid.
4. ElGamal encryption use a random integer r for each message, what will happen if r is used twice?

send the solutions to gracehgs@mail.sjtu.edu.cn

Deadline: May 19th